20190110O - Shubham Patel

Page No.: 1

SC402 - Homework 4

Date:

[1] Here, $2^{48} \bmod 97 = 1$

$3^{48} \bmod 97 = 1$

$4^{48} \bmod 97 = 1$

$5^{48} \bmod 97 = 96$

and $5^{32} \bmod 97 = 35$

So, the smallest primitive element modulo 97 is 5.

[2] For, $n = pq$ ip and q are distinct odd primes

$$\lambda(n) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)}$$

(a) Denote $d = \gcd(p-1, q-1)$, $p-1 = p'd$ and $q-1 = q'd$

Then, $\lambda(n) = p'q'd = (p-1)q' = p'(q-1)$

We have, $ab \equiv 1 \pmod{\lambda(n)}$,

$ab = k(\lambda(n)) + 1 = k(p-1)q' + 1$

Then,

$$x^{ab} \equiv x^{k(p-1)q'+1} \pmod{p} \equiv x \pmod{p}$$

Similarly, $x^{ab} \equiv x^{k(q-1)p'+1} \pmod{q} \equiv x \pmod{q}$

Since, $x^{ab} \equiv x \pmod{p}$ mod $x^{ab} \equiv$ mod q.

It follows that $x^{ab} \equiv x \pmod{n}$

(b) $d = 6$, $\lambda(n) = 468$ and $\phi(n) = 2808$
$b^{-1} \bmod \lambda(n) = 67$ and $b^{-1} \bmod \phi(n) = 2407$

[3] $28702 = (2)^1 \times (113)^1 \times (127)^1$

we find that,
$\log_5 8563 \equiv 1 \pmod 2$,
$\log_5 8563 \equiv 67 \pmod{113}$ and $\log_5 8563 \equiv 99 \pmod{127}$

- By chinese reminder theorem,
$\log_5 8563 \equiv 3903$

→ $31152 \equiv (2)^4 \times (3)^1 \times (11)^1 \times (59)^1$
we find that, $\log_{10} 12611 \equiv 14 \pmod{16}$,
$\log_{10} 12611 \equiv 2 \bmod (3)$, $\log_{10} 12611 \equiv 8 \pmod{11}$
and $\log_{10} 12611 \equiv 51 \pmod{59}$

By chinese reminder theorem,
$\log_{10} 12611 = 17102$.

[4] (a) Points on the elliptic curve $y^2 = x^3 + x + 28$ define over Z_{71}

We make table of x, $x^3 + x + 28 \bmod 71$ quadratic residue and y points

We get 72 number of points by doing that.

(b) If E were cyclic, there would be points having order 72 but there are no such points.

(c) The maximum order of point is 36.
(4, 5) is a point having order 36.
[E is isomorphic to $Z_{36} \times Z_2$]

[5] First,

$$k = (x_1 - x_2)(s_1 - s_2)^{-1} \bmod (p-1)$$
$$= -22425 \times 10915^{-1} \bmod 31846$$
$$= 1165$$

- To determine 'a', we will solve congruence,

$$r_a = x_1 - ks_1 \pmod{p-1}$$

For 'a', this congruence simplifies to,

$$23972\,a \equiv 23704 \pmod{31846}$$

- we have, gcd (23972, 31846) = 2 and 2 | 23704, so congruence is equivalent to,

$$11986\,a \equiv 11852 \pmod{15923}$$

- This congruence has solution,

$$a \equiv 11852 \times 11986^{-1} \pmod{15923}$$
$$\equiv 7459 \pmod{15923}$$

- So, $a = 7459$ or $a = 7459 + (p-1)(2)$
$= 23382$

- By computing $\alpha^{7459} \bmod p = 25703 = \beta$ and $\alpha^{23382} \bmod p = 6144 \neq \beta$, we see that,

$\alpha = 7459$

[6] (a) Signature (20679, 11082) on the message $x = 20543$.

$5^{20543} \bmod 31847 = 20688$

$= 26379^{20679} \; 20679^{11082} \bmod 31847$

(b) By solving instance of discrete logarithm,

$a = \log_5 26379 = 7973$

(c) To determine 'k', we solve the congruence,

$k s \equiv x - ar \pmod{p-1}$

- for, k. This congruence simplifies to,
  $11082\,k \equiv 13618 \pmod{31846}$
- $\gcd(11082, 31846) = 2$
- and $2 \mid 13618$, so congruence is equivalent to $5541\,k \equiv 6809 \pmod{15923}$
- this congruence has the solution,
  $k \equiv 6809 \times 5541^{-1} \pmod{15923} \equiv 3464 \pmod{15923}$
- Therefore, $k = 3464$ or $k = 7459 + (p-1)/2 = 19387$.

By computing $\alpha^{3464} \bmod p = 11168 \neq r$ and $\alpha^{19387} \bmod p = 20679 = r$, we see that, $k = 19387$.